UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/997,012	11/30/2001	Jeeyeon Kim	3882-0102P	7257

2292 7590 03/31/2005

BIRCH STEWART KOLASCH & BIRCH
PO BOX 747
FALLS CHURCH, VA 22040-0747

EXAMINER	
HENNING, MATTHEW T	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 03/31/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/997,012	KIM ET AL.	
	Examiner	Art Unit	
	Matthew T Henning	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 November 2001*.

2a)☐ This action is FINAL. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☒ Claim(s) *1-3,5-13,15 and 16* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 November 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *11/30/2001*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other. _____.

This action is in response to the communication filed on 11/30/2001.

1. Claims 1-16 have been examined.

Title

2. The title of the invention is acceptable.

Priority

3. The application has been filed under Title 35 U.S.C §119, claiming priority to Korean application 10-2001-0019279, filed 4/11/2001.

4. The effective filing date for the subject matter defined in the pending claims in this application is 4/11/2001.

Information Disclosure Statement

5. The information disclosure statement (IDS) submitted on 11/30/2001 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statement.

Drawings

6. The drawings filed on 11/30/2001 are acceptable for examination proceedings.

Specification

7. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

8. The abstract of the disclosure is objected to because

Lines 1 and 8: The phrase "The present invention discloses" can be implied and therefore must be removed.

The abstract is objected to for containing multiple paragraphs.

Correction is required. See MPEP § 608.01(b).

9. The disclosure is objected to because it contains an embedded hyperlink and/or other form of browser-executable code. Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code. (See pages 4 and 7 of the specification).

See MPEP § 608.01. Appropriate correction is required.

10. The listing of references in the specification is not a proper information disclosure statement. 37 CFR 1.98(b) requires a list of all patents, publications, or other information submitted for consideration by the Office, and MPEP § 609 A(1) states, "the list may not be incorporated into the specification but must be submitted in a separate paper." Therefore, unless the references have been cited by the examiner on form PTO-892, they have not been considered.

Claim Objections

11. Claims 1-3, 5-13, and 15-16 are objected to because of the following informalities:

12. Claims 1-2 contains multiple terminating periods.

13. Claim 3 is objected to by virtue of its dependency to claim 2.

14. Claim 5 Line 4 recites "KRA" to refer to the key management authority, which should be "KMA".

15. Claim 12 Line 7 recites "(C = E_{PWD} (PRI)" which should have one more parenthesis.

16. Claims 6-11, 13, and 15-16 are objected to by virtue of their dependency to claim 5 or 12.

17. Appropriate correction is required.

Claim Rejections - 35 USC § 112

18. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

19. Claims 1-16 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

20. A broad range or limitation together with a narrow range or limitation that falls within the broad range or limitation (in the same claim) is considered indefinite, since the resulting claim does not clearly set forth the metes and bounds of the patent protection desired. Note the explanation given by the Board of Patent Appeals and Interferences in *Ex parte Wu*, 10 USPQ2d 2031, 2033 (Bd. Pat. App. & Inter. 1989), as to where broad language is followed by "such as" and then narrow language. The Board stated that this can render a claim indefinite by raising a question or doubt as to whether the feature introduced by such language is (a) merely exemplary of the remainder of the claim, and therefore not required, or (b) a required feature of the claims. Note also, for example, the decisions of *Ex parte Steigewald*, 131 USPQ 74 (Bd. App. 1961); *Ex parte Hall*, 83 USPQ 38 (Bd. App. 1948); and *Ex parte Hasche*, 86 USPQ 481 (Bd. App. 1949). In the present instance, claims 1, 2, and 4 recite the broad recitation, encrypting the private key with a password", and the claim also recites "i.e. $C = E_{PWD}$ (PRI), where PWD is user's password and PRI is user's private key" which is the narrower statement of the range/limitation. It would be unclear to the ordinary person skilled in the art at the time of

invention whether this limitation was meant to be limited to encrypting the private key only with the password, or whether encrypting the private key with the password and a secret key would also fall within the scope of the claim. As such, one of ordinary skill in the art would be unable to determine the scope of the claim. Therefore, claims 1, 2, and 4 fail to particularly point out and distinctly claim the subject matter which the applicants regard as the invention.

21. Claim 3 is rejected by virtue of its dependency to claim 2.

22. Claim 5 recites the limitation "the corresponding user" in line 5. There is insufficient antecedent basis for this limitation in the claim.

23. Claim 6 recites the limitation "the court" in line 4. There is insufficient antecedent basis for this limitation in the claim.

24. Claim 7 recites the limitation "less than all of shares of the corresponding user's key recovery block" in lines 2-3. There is insufficient antecedent basis for this limitation in the claim.

25. Claim 9 recites the limitation "the password-based private key downloading protocol" in lines 4-5. There is insufficient antecedent basis for this limitation in the claim.

26. Claims 6-11 are rejected by virtue of their dependency to claim 5.

27. Claim 11 recites the limitation "the user's registered passwords" in 4. There is insufficient antecedent basis for this limitation in the claim.

28. Claim 12 recites the limitation "the divided shares" in lines 11-12. There is insufficient antecedent basis for this limitation in the claim.

29. Claim 13 recites the limitation "the validity" in line 3. There is insufficient antecedent basis for this limitation in the claim.

30. Claim 14 recites the limitation "the divided shares" in lines 11-12. There is insufficient antecedent basis for this limitation in the claim.

31. Claim 14 recites "comprising" in both lines 2 and 4. The ordinary person skilled in the art would be unable to determine whether the preamble includes lines 3-4 or not. Therefore, claim 14 is rejected for failing to particularly point out and distinctly claim the subject matter which the applicants regard as the invention.

32. Claim 14 recites the limitation "a KMA" in both line 4 and line 5. The ordinary person skilled in the art would be unable to determine whether the second recitation was meant to establish a second KMA or was meant to refer to the first. Therefore, claim 14 is rejected for failing to particularly point out and distinctly claim the subject matter which the applicants regard as the invention.

33. Claims 15-16 are rejected by virtue of their dependency to claims 12 and 14.

Claim Rejections - 35 USC § 102

34. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> *A person shall be entitled to a patent unless –*
>
> *(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.*
>
> *(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the*

international application designated the United States and was published under Article 21(2) of such treaty in the English language.

35. Claims 1-3, 12-13, and 15-16 are rejected under 35 U.S.C. 102(e) as being anticipated by Micali (US Patent RE. 36,918).

36. Regarding claim 1, Micali disclosed a method, under the PKI environment, of the key generation and escrow (See Micali Col. 2 Paragraph 8), comprising the steps of: (a) having the user generate a password and register a password verifier of the user in a key management authority (See Micali Col. 11 Paragraph 6); (b) having the user generate a pair of private/public keys (See Micali Col. 4 Paragraph 3); having the user encrypt his own private key with his own password (See Micali Col. 11 Paragraph 6); (d) having the user generate a key recovery block through encryption of the encrypted private key C with a public key of a key recovery agents (See Micali Col. 10 Paragraph 4); (e) sending user's key recovery block and public key to the key management authority (See Micali Col. 4 Lines 45-47); and (f) having the key management authority store the key recovery block, or divide it into several shares, followed by storing the shares separately (See Micali Col. 4 Lines 45-57).

37. Claim 2 is rejected for the same reasons as claim 1 above and further because Micali disclosed checking the validity of the key recovery block (See Micali Col. 4 Lines 39-57).

38. Regarding claim 3, Micali disclosed not encrypting the private key with a password and generating a key recovery block through the encryption of said user's private key with a public key of a key recovery agent by said user (See Micali Col. 4 Lines 45-47 and Col. 10 paragraph 4).

39. Regarding claim 12, Micali disclosed a key escrow system for the PKI environment comprising: a user who generates his own password, registers his own password verifier in a key management authority (KMA), generates a pair of private/public key pairs (PRI, PUB), encrypts his private key with said password, and generates a key recovery block (KRB) through encrypting C with a public key of key recovery agents (KRAs) (See rejection of claim 1 above), a KMA that stores either said KRB or the divided shares of said KRB in a distributed manner, constructs said KRB from the divided shares at a key recovery phase, sends to KRAs a request for the key recovery along with a blinded KRB which is a multiplication of said KRB with a blind factor in order not to disclose said KRB to any of said KRAS, and recovers C with received messages from said KRAS and with said blind factor (See Micali Col. 10 Paragraphs 3-6); and KRAs that decrypt message sent from said KMA with the private key of their owns (See Micali Col. 10 Paragraph 4).

40. Regarding claim 13, Micali disclosed that KRB generated by said user is checked for the validity (See Micali Col. 10 Paragraphs 4-5).

41. Regarding claim 15-16, Micali disclosed that not all the shares were required to reconstruct the key (See Micali Col. 9 Paragraph 2).

42. Claim 4 is rejected under 35 U.S.C. 102(e) as being anticipated by Al-Salqan (US Patent Number 6,549,626).

Al-Salqan disclosed a method, under the PKI environment, of the key generation and escrow (See Al-Salqan Abstract), comprising the steps of: (a) having the user register his password in a key management authority (KMA) (See Al-Salqan Col. 4 Paragraphs 2-3); (b) having the KMA generate a pair of private/public keys for the user (See Al-Salqan Col. Line 53

– Col. 4 Line 7); (c) having the KMA encrypt the user's private key with the registered password of the user (See Al-Salqan Col. 4 Lines 29-61); (d) having the KMA generate a key recovery block(KRB) through the encryption of said encrypted private key C with a public key of a key recovery agents (KRAs) (See Al-Salqan Col. 4 Line 62 – Col. 5 Line 5); and (e) having the KMA either to store the KRB, or to divide the KRB into several shares, followed by separately storing said shares (See Al-Salqan Col. 5 Paragraph 1).

43. Claims 5-6 are rejected under 35 U.S.C. 102(b) as being anticipated by Dabbish et al. (US Patent Number 5,917,911) hereinafter referred to as Dabbish.

44. Regarding claim 5, Dabbish disclosed a method, under the PKI environment, of the key recovery (See Dabbish Abstract), comprising the steps of: (a) having a key management authority (KRA) construct a key recovery block (KRB) for the corresponding user upon the request for the key recovery (See Dabbish Col. 6 Lines 19-31); (b) having the KMA to blind the constructed key recovery block by employing a blind factor of said key management authority's own so that any KRA is not able to see said constructed key recovery block (See Dabbish Col. 7 Paragraph 6); (c) having the KMA to send the blinded key recovery block along with a request for the key recovery to KRAs (See Dabbish Col. 7 Paragraph 5); (d) having each KRA perform a decryption of the message received by employing a private key of its own (See Dabbish Col. 8 Paragraph 4); (e) having each KRA send the decrypted message processed at step (d) to said key management authority (See Dabbish Col. 7 Paragraph 6); and (f) having the KMA recover a encrypted private key C of said user by employing the message received from each key recovery agent and said blind factor of its own (See Dabbish Col. 8 Paragraph 6).

45. Regarding claim 6, Dabbish disclosed that the request for the key recovery at step (a) is the request either from said user or from the court (See Dabbish Col. 5 paragraphs 4-5).

Claim Rejections - 35 USC § 103

46. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> *(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.*

47. Claims 7-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dabbish as applied to claim 5 above, and further in view of Micali.

48. Regarding claims 7and 8, Dabbish disclosed providing split key recovery (See Dabbish Col. 9 Paragraph 4), but failed to disclose that not all the shares of the recovery block or all the messages from the split agents were required to recover the key.

Micali teaches a system in which split key recovery does not require all the shares of the recovery block, and therefore not all the messages containing the shares, in order to recover the key (See Micali Col. 9 Paragraph 2).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Micali in the split key recovery system of Dabbish by only requiring a portion of the shares in order to recover the key. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect the system from untrustworthy share holders who do not provide the requested share.

49. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Dabbish as applied to claim 5 above, and further in view of Al-Salqan.

Dabbish disclosed a key recovery system (See the rejection of claim 5 above), but failed to disclose the recovered key being encrypted by a user's registered password.

Al-Salqan teaches a method for protecting a user's key in a recovery system by password encrypting the key and then using the password to decrypt the key upon recovery (See Al-Salqan Col. 4 Paragraphs 2-5 and Col. 6 Paragraphs 4-5).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Al-Salqan in the key recovery system of Dabbish by encrypting the key with a password and then using the password to decrypt the key upon recovery. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect the key against security breaches at the KMCs.

50. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Dabbish and Al-Salqan as applied to claim 11 above, and further in view of Schneier ("Applied Cryptography").

The combination of Dabbish and Al-Salqan disclosed recovering a password encrypted key upon request (See the rejection of claim 11 above), but failed to disclose mounting a dictionary attack on the encrypted key in order to decrypt the key.

Schneier teaches a method for decrypting password-encrypted files called a dictionary attack (See Schneier Pages 171-173).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Schneier in the key recovery system of Dabbish and Al-

Salqan by mounting a dictionary attack on the password encrypted key in order to decrypt the key. This would have been obvious because the ordinary person skilled in the art would have motivated to protect against the password being forgotten or lost.

51. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Dabbish as applied to claim 5 above, and further in view of Perlman et al. ("Password-Based Private-Key Download Protocols") hereinafter referred to as Perlman.

Dabbish disclosed a system for key recovery in which a key is recovered and sent to a user (See the rejection of claim 5 above) but failed to disclose using a password-based private key download protocol in order to receive the recovered key.

Perlman teaches that by a using a password-based private key download protocol to download a private key, an eavesdropper gains no information about the key (See Perlman Page 10).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Perlman in the key recovery system of Dabbish by using a password-based private key download protocol to download the recovered private key. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect against an eavesdropper discovering the recovered key.

52. Claims 14-16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Al-Salqan as applied to claim 4 above, and further in view of Micali.

Al-Salqan disclosed a key escrow system for PKI environment comprising: a user who registers his password (PWD) in a key management authority (KMA), comprising: a KMA that generates a pair of private/public keys (PRI, PUB) for said user, encrypts said user's private key

with said user's registered password, generates a key recovery block (KRB) through encrypting C with the public key of the key recovery agents (KRAs), stores said KRB (See the rejection of claim 4 above), but failed to disclose splitting the storage of the KRB, requiring only a portion of the shares to recover the block from the distributed storage and sending messages to be decrypted with private keys of their own to the recovery agents.

Micali teaches that in a key recovery system, the key should be split and stored with separate agents such that more than one agent is needed to recover the key but not all the agents are needed to recover the key (See Micali Col. 9 Paragraph 2). It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Micali in the key recovery system of Al-Salqan by splitting the recovery block and storing it among different agents as well as only requiring some of the shares in order to recover the key. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide protection against corrupt and uncooperative key stores.

Micali further teaches that recovery messages should be sent blindly to the agents and that the share messages should be sent encrypted with the public key of the agent and decrypted with the private key of the agent (See Micali Col. 10 Paragraphs 3-6). It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Micali in the key recovery system by sending the recovery request blindly to the agents and sending the shares encrypted with the public key of the agent. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect against the illicit collection of the recovery shares and the release of the identity of the key owner.

Conclusion

53. Claims 1-16 have been rejected.

54. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Denning et al. ("A Taxonomy for Key escrow Encryption Systems") disclosed many different features of escrow systems and which systems utilize which features.

55. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Matthew Henning
Assistant Examiner
Art Unit 2131
3/29/05

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100